

PCT

REC'D 07 JUN 2004

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL  
(article 36 et règle 70 du PCT)



PCT

Référence du dossier du déposant ou du mandataire	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/PEA/416)	
Demande Internationale No. PCT/IB 03/02425	Date du dépôt international (jour/mois/année) 10.06.2003	Date de priorité (jour/mois/année) 12.06.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/08		
Déposant NAGRACARD SA et al.		

- Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
- Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.  
  
☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).  
  
Ces annexes comprennent feuilles.

- Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :

- I ☒ Base de l'opinion
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 20.12.2003	Date d'achèvement du présent rapport 07.06.2004
Nom et adresse postale de l'administration chargée de l'examen préliminaire international   Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé  Holper, G  N° de téléphone +31 70 340-2304  

PCT/B 03/02425

**RAPPORT D'EXAMEN  
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n°

PCT/IB 03/02425

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

*(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)*

6. Observations complémentaires, le cas échéant :

**V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

1. Déclaration

Nouveauté	Oui:	Revendications	1-16
	Non:	Revendications	
Activité inventive	Oui:	Revendications	1-16
	Non:	Revendications	
Possibilité d'application industrielle	Oui:	Revendications	1-16
	Non:	Revendications	

2. Citations et explications

**voir feuille séparée**

**BEST AVAILABLE COPY**

**Concernant le point V**

**Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

Il est fait référence au document suivant:

D1: WO 97/38530 (DIGCO)

La présente demande concerne un procédé d'échange sécurisé d'informations localement connectés entre eux ainsi qu'un récepteur pour la mise en oeuvre du dit procédé.

L'état de la technique le plus proche est illustré par D1 qui divulgue un procédé d'échange sécurisé d'informations entre un récepteur et un module de sécurité, les deux dispositifs étant localement connectés. Le récepteur comporte une clé publique tandis que le module de sécurité comporte une clé privée correspondante. Le procédé sert à échanger une clé de session aléatoire chiffrée par la clé publique.

Problème dans l'état de la technique: la clé de session peut être imposée par un intrus qui utiliserait ainsi une lacune de sécurité du procédé.

Selon la revendication 1 ce problème est résolu par les étapes consistant à générer un nombre aléatoire différent dans chaque dispositif, chiffrer ce nombre par la première respectivement la seconde clé de la paire de clés, transmettre le nombre chiffré à l'autre dispositif, déchiffrer les nombres chiffrés dans chaque dispositif et combiner lesdits nombres aléatoires pour générer une clé de session utilisée pour l'échange de données entre les deux dispositifs.

Un procédé basé sur le chiffrement de deux nombres aléatoires chiffrés par deux clés différentes de la même paire de clés n'est pas connu ni suggéré par l'état de la technique.

La revendication 1 remplit donc les critères de nouveauté et d'activité inventive de l'article 33(2) et (3) PCT.

Le récepteur selon la revendication 15 est arrangé pour la mise en oeuvre du procédé selon la revendication 1 et remplit donc aussi les critères de nouveauté et d'activité

**BEST AVAILABLE COPY**

inventive.

Les caractéristiques supplémentaires des revendications dépendantes 2-14 et 16 définissent des détails de réalisation de sorte que ces revendications sont aussi nouvelles et inventives.

Les procédés et récepteurs revendiqués présentent la possibilité d'activité industrielle.

**BEST AVAILABLE COPY**